



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/884,672	06/19/2001	Tetsuya Noguchi	JP920000134US1	4503

7590 08/21/2006

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. Box 218
YORKTOWN HEIGHTS, NY 10598

[REDACTED] EXAMINER

POLTORAK, PIOTR

[REDACTED] ART UNIT [REDACTED] PAPER NUMBER

2134

DATE MAILED: 08/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/884,672	NOGUCHI ET AL.
Examiner	Art Unit	
Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 June 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-4,6-16,18-28 and 30-41 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-4,6-16,18-28,30-41 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. The Amendment, and remarks therein, received on 6/14/06 have been entered and carefully considered.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

3. Applicant's arguments have been carefully considered but they were not found persuasive.
4. Applicant asserts that the new amendments introduced to the claim language overcome 35 USC § 112 second paragraph rejection.
Although the amendments addressed most of the issues the examiner points out that
5. From applicant's argument it appears that applicant attempts to underline the fact that the outputted first verification data (*SRES*) is compared with the outputted second verification data (*SRES'*). However, the claim limitations: "it is determined whether the verification data at the first and second verification data output sections match mutually" reads on Vainio's teaching, which disclose a copy of the second verification data that is received by the first data send/receive device that determines whether *SRES=SRES'*.
6. As per claims 1, 13, 25 and 30-41 applicant argues that Vainio reference does not teach "that two send/receive devices generate verification data and send that data to their respective output devices, after which the data are compared". Applicant

follows with the allegation that contrary to examiner's statement in the previous Office Action, claims clearly recite that "the first device generates first verification data and places it in a first verification data output section and that the second device generates second verification data and places it in a second verification data output section".

The examiner points out that the language as recited (above) by applicant has been introduced (to clarify applicant's intention) by amendments. Furthermore, the examiner considers that the section outside of segment implementing E1 algorithm to be verification data output section. In Fig. 6 Vainio clearly discloses that "the first device generates first verification data and places it in a first verification data output section and that the second device generates second verification data and places it in a second verification data output section".

7. As per claims 1, 13, 25 and 30-41 applicant also argues the 35 USC § 102 rejection stating that "generation of verification data by more than one user device is neither taught nor suggested".

Applicant's argument is not understood. Fig. 6 clearly shows two devices generating verification data after which determination whether two verification data match ($SRES? = SRES'$).

8. As per the following argument that Vainio does not teach or suggests that a plurality of verification data values be generated and compared for mutual matches the examiner points out that, as noted in the previous Office Action, Vainio's invention is a generic discussion clearly intended for multiple use in multiple devices and as a

result the authentication scheme as disclosed in Fig. 6 is repeated numerous times resulting in generation of a plurality of verification data values that is then matched ($SRES? = SRES'$). For example, in the “2.1 Background” Vainio highlights the aim of its invention: “Bluetooth can be used to connect almost any device to another device”. The fact that Vainio’s invention is implemented in communication between a plurality of devices is also evidenced in “Security in AdHoc Network” section, where Vainio explicitly recites: “all the devices on an ad hoc network connect to each other via wireless links” and Fig. 1, for example, that explicitly illustrates that the subject of the invention is a plurality of devices.

As discussed above communication between two devices results in each of the first algorithms of a first and second devices to generate verification data and in determination whether the verification data at the first and second verification data output match mutually ($SRES? = SRES'$). Thus, Fig. 1 multiple device communication results at least in one of the device communicating with a plurality (more than one) of devices, which will result in a plurality of verification data, wherein for each one of them it will be determined whether the verification data at the first (initiator) and second (responder) verification data output sections match mutually. Thus, each one of the devices disclosed in Fig. 1 produces at least a set of two verification data (Device A generate a set of verification data: one during communicating with Device B and another with Device C, Device B generates verification data during communication with Device C and Device A and Device C generates verification data while communicating with Device A and B).

9. Applicant arguments directed towards claims 2-3, 14-15 and 26-27 are essentially directed towards the stated above, alleged shortcoming of art of record. As a result the arguments are also not found persuasive.

10. As per claims 4, 6-8, 10, 12, 16, 18-19 applicant argues that Schneier "does show hash functions but does not teach or suggests a serial sequence of operators that are composed of more than one operators arranged in series wherein the operators relate to the same or different one-way functions" and that an output from the serial sequence of operators is the verification data.

The argument is not understood especially since Fig. 18.2 disclosed by Schneier alone clearly discloses "a serial sequence of operators that are composed of more than one operators arranged in series wherein the operators relate to the same or different one-way functions" and applicant does not provide any clear arguments to the contrary. Additionally, the examiner reminds applicant that Schneier's reference was not to substitute but rather to complement Vanio's reference that discloses the verification data.

11. As per claims 8-9, 11, 13-15, 20-21, 23, 33, 35, 38 and 40 applicant repeats previously stated arguments directed towards previously argued claims. Applicant's arguments have been carefully considered but they were not found persuasive. See the examiner response to the previous claims, above.

12. As per claims 8, 13-15, 20 and 25-27 applicant argues that Hind reference does not teach displaying and verifying a device identifier. The argument is not understood since argued claims do not include the argued limitation.

13. Lastly, as per claims 8, 13-15, 20 and 25-27 applicant argues that Vainio in view of Hind does not disclose that verification data in visual and auditory form.

14. The examiner respectfully disagrees and points the examiner to previously paragraph 70 in the previous Office Action.

15. Claims 1-4, 6-16, 18-28 and 30-41 have been examined.

Claim Rejections - 35 USC § 102

16. Claims 1, 13, 25, 30-31 and 37 remains rejected under 35 U.S.C. 102(e) as being anticipated by Vainio (Juha T. Vainio, "Bluetooth Security").

Vainio teaches sending data for verification data generation (RAND A) from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection (*In Vanios' Bluetooth authentication scheme a Device A sends RAND A to a Device B. 5.3 Authentication, in particular Fig. 6*).

Vainio teaches in the first data send/receive device, generating verification data (SRES') from the sent data for verification data generation produced using a first generation algorithm (E1) and outputting the generated verification data (5.3 *Authentication, illustrated by Fig. 1, in particular the Device A*).

Vainio also teaches in the second data send/receive device, generating verification data (SRES) from the received data for verification data generation produced using the first generation algorithm (E1) and outputting the generated verification data to

the first verification data output section (*5.3 Authentication, illustrated by Fig. 1, in particular the Device B*).

Vainio teaches determining whether the verification data at the first and second verification data output sections match mutually (*SRES' ?= SRES, Fig. 6*).

17. Vainio's invention is a generic discussion clearly intended for multiple use in multiple devices and as a result the authentication scheme as disclosed in Fig. 6 is repeated numerous times resulting in generation of a plurality of verification data values that is then matched (*SRES?=SRES'*). As discussed in the Response to Amendment section above, Vainio's exchange shown in Fig. 6 implemented in communication of plurality of devices as shown in Fig. 1, results in the first generation algorithm generating a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.

18. Claims 1, 25 and 30-31 are substantially equivalent to claim 13; therefore claims 1, 25 and 30-31 are similarly rejected.

Claim Rejections - 35 USC § 103

19. Claims 2-3, 14-15 and 26-27 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Vainio (*Juha T. Vainio, "Bluetooth Security"*) in view of Kuwamoto et al. (EP 0919945).

Vainio teaches an ad-hoc radio communication as discussed above.

Vainio does not explicitly teach that the verification data is visual and auditory verification data.

20. *Kuwamoto et al.* teach visual and auditory verification data [39].

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize visual and auditory verification data in Vainio's invention given the benefit of usability.

21. In addition, the examiner also points out that the form of visual or auditory verification data are well known in the art. For example the correct transfer of data during synchronizing hand held devices (e.g. PALMS) with other devices (e.g. computers) is frequently verified by visual or auditory check of the sending and receiving device.

22. Claims 4, 6-8, 10, 12, 16, 18-20, 22, 24, 28, 32, 34, 39 and 41 remain rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)*.

Vainio teaches a method and a system including a first generation algorithm (*E1*) that given input of the data for verification data generation outputs the verification data as discussed above.

23. As per claims 4, 6-7, 16, 18-19 Vainio does not teach that the first generation algorithm comprise a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way function.

24. Schneier's discloses a serial sequence of operators that are composed of more than one operators arranged in series that are related to the same or different one-way function (pg. 351-353 and 433-438).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate of more than one operators arranged in series that are related to the same or different one-way function as taught by Schneier into the first generation algorithm as taught by Vainio. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase system's security.

25. As per claims 4, 6-7, 16, 18-19 Vainio does not teach the encryption E0 for verification data generation is operated by the serial sequence of operators

26. As per claims 8 and 20 Vainio does not explicitly teach transmitting a public key between the portable devices.

27. Schneier teaches transmitting a public key from a sender and a receiver to allow secure communication (*Alice and Bob, "2.5 Communications using public-key cryptography"*, pg. 31-32). However, Schneier warns about "man-in-the-middle attacks" (pg. 48-49).

Vainio teaches sending data for verification data generation (*RAND A*) from a sender to a receiver that allows generating verification data (*SRES*). The verification data is derived from additional data that is unique to the recipient (*Vainio Fig. 6*) and is sent back for verification to the sender. This scheme decreases chances of "man-in-the-middle attacks".

Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to transmit the public key from one portable terminal to another as taught by Schneier as the data for verification data generation as taught by Vainio. One of ordinary skill in the art would have been motivated to perform such a modification in order to secure data exchange between portable terminals (*solving a key-management problem*) while minimizing man-in-the-middle attacks.

28. As per claims 10, 12, 22 and 24 Vainio teaches that one of the portable terminals receive information and using the information (*and second generation algorithms E21, E22*) produces a symmetric key Kc (*Fig. 2 and 3*). Vainio explicitly teach that Kc is produced on both portable terminals (*Vainio talks about the key exchange process, pg. 8*). The information comprise a random number (*RandD*) and it is implicit that they also must comprise information identifying the second generation algorithm in order for the key exchange parties to know which of the algorithms was used in order to derive the identical Kc.

Vainio does not explicitly teach that the Kc is sent from the portable terminal to the personal computer of each user and the personal computers exchanging data in cipher using the symmetric key Kc.

29. Official Notice is taken that it is old and well-known practice to communicate data from a portable terminal to a personal computer (e.g. U.S. Pub. No. 20010013890). One of ordinary skill in the art at the time of applicant's invention would have been motivated to extend personal computer's capability by data easily obtained using a

- portable device as well as extend the portable terminals that have limited resources such as memory.
30. Also Official Notice is taken that it is old and well-known practice to use personal computers to send and receive data in cipher using symmetric keys. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ secure data communication between personal computers.
31. Schneier teaches that the cipher key should be done using other communication channels than cipher data exchange (*Schneier, pg. 176, last three §-pg. 177, first two §*) and using portable terminals (*as taught by Vainio*) as "other communication channels" would have been an obvious choice given the benefit of portability and "man-in-the-middle" attack prevention mechanism.
32. Claims 9, 11, 21, 23, 33, 35, 38 and 40 remain rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)* and in further view *Lin (U.S. Pub. 20020025046)*.
- Claims 9, 11, 21 and 23 are essentially identical to claims 10, 12, 22 and 24 discussed above with the exception that the symmetric Kc is computed on the personal computers rather than portable terminals.
33. Lin teaches that computing power, memory capacity and supply power of the portable device may not be sufficient for key generation (*Lin, [21]*). Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to modify Vainio's invention in order to generate the keys Kc on the personal computers. One of ordinary skill in the art would have been motivated to perform such a modification in order to move key generation into the higher power and memory capacity devices.

34. Claims 1-3, 8, 13-15, 20 and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Hind et al. (U.S. Pub. No. 6772331)*.

As per claims 1, 13 and 25 Hind et al. teach sending data for verification data generation (certificate 6030) from one data send/receive device to the other send/receive device (6001/6003), wherein the two send/receive devices are mutually connected by an ad-hoc radio connection (col. 9 lines 16-20 and fig. 6) upon which verification data (*the identifier of the sending device*) is displayed and verified that matches mutually (col. 13 lines 17-26).

35. Hind et al. teach that the verification data is generated by a first generation algorithm (col. 12 lines 3-5).

36. As per claims 2-3, 14-15 and 26-27- Hind et al. teach that the verification data is the visual and auditory form (col. 13 lines 17-26).

37. As per claims 8 and 20 the data for verification data generation comprise public key (fig. 4).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

8/15/06


Jacques Louis-Jacques
JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100